ACADEMIC PRESS

Available at WWW.MATHEMATICSWEB.ORG POWERED BY SCIENCE @ DIRECT®

Journal of Algebra 265 (2003) 539–561

JOURNAL OF Algebra

www.elsevier.com/locate/jalgebra

Algebraic observations on the Jacobian conjecture

Eloise Hamann

Department of Mathematics, San Jose State University, San Jose, CA 95192-0103, USA

Received 14 November 2001

Communicated by Craig Huneke

Abstract

This paper contains conditions that are equivalent to the Jacobian Conjecture (JC) in two variables and partial results toward establishing these conditions. If u and v are a Jacobian pair of polynomials in $k[x, y]$ which provide a counterexample then by a change of variables there is a Jacobian pair which generate an ideal of the form $\langle p(x), y\rangle$. (A similar result holds for an arbitrary number of variables.) JC follows if $p(x)$ must be linear or equivalently if $p'(x)$ is constant. Conditions which yield this result are derived from the Jacobian relation and the fact that $\langle u, v\rangle = \langle p(x), y\rangle$. Other conditions that imply JC are derived from the fact that JC follows if the ring $k[x, u, v] = k[x, y]$ when the Jacobian determinant of u and v is 1. One easily arranges for $k[x, y]$ to be integral over $k[x, u, v]$ with the same quotient fields. For example, if $k[x, u, v]$ must be square-root closed in $k[x, y]$, JC follows. The paper studies the case where $j(u, v) = 1$ forces $k[x, u, v]$ to be seminormal in $k[x, y]$. In this case and in other cases, y satisfies a monic polynomial of degree two over a localization of $k[x, u, v]$. Conditions that imply $k[x, u, v] = k[x, y]$ include equality after taking quotient rings and localizing. Other conditions which imply equality involve showing $k[x, u, v]$ is a regular ring and computation of the conductor ideal which must be principal as an ideal of $k[x, y]$.

0. Introduction

0.1. An ideal theoretic formulation of JC, and form of the ideal generated by polynomials with Jacobian one

The usual statement of the Jacobian Conjecture, abbreviated as JC, is:

E-mail address: hamann@math.sjsu.edu.

0021-8693/03/$ – see front matter
doi:10.1016/S0021-8693(03)00226-6

JC1: Let k be a field of characteristic zero and F a polynomial map, $F : k^n \to k^n$, then if the Jacobian determinant, $j(F) \in k^*$, F is invertible.

JC2: JC1 follows if $j(F) \in k^*$ implies F is one to one when k is algebraically closed [BCW].

The conjecture is easily seen to be equivalent to:

JC3: Let k be a field of characteristic 0 and $\{F_1, \ldots, F_d\}$ a set of polynomials from $k[X_1, \ldots, X_n]$ over k. If $j(F_1, \ldots, F_d) \in k^*$, then $k[F_1, \ldots, F_d] = k[X_1, \ldots, X_d]$.

The bibliography of *Polynomial automorphisms and the Jacobian Conjecture* [vdE], by Arno van den Essen contains an extensive list of papers on the problem. The paper by Bass, Connell, and Wright [BCW] remains a notable source for the approaches to JC and includes the reduction to degree 3 if the number of variables is arbitrary. The two-variable Case has been of particular interest and probably inspired the famous paper, *Embeddings of lines in the plane*, by Abyhankar and Moh who have significant results in this case [AM]. Thanks are due to Richard Swan for his comments on a preprint of this paper.

We assume throughout that k is algebraically closed since it is known that if it is true for one field of characteristic 0, it is true in general [BCW].

Conditions which imply the Jacobian Conjecture for a polynomial ring $S = k[x, y]$ over a field k of characteristic 0 are described in this paper. The reader may appreciate the following overview.

0.2. Overview

One set of conditions which imply JC is related to the easy result that if the ideal generated by a set of n polynomials in n variables whose Jacobian determinant is 1, must be a maximal ideal then JC follows. By a change of variables, one may assume the ideal in question is generated by $n - 1$ of the variables and a polynomial $p(x_1)$ in the remaining variable. Thus, it suffices to prove the polynomial p is linear or that its derivative, p', is a constant. One can achieve some reduction of degree with this setup by using a trick of David Wright which increases the number of variables. Section one deals with the case of two variables with the Jacobian determinant, $j(u, v) = 1$, where the ideal $I = \langle u, v\rangle = \langle p(x), y\rangle$ in $k[x, y]$. It is easy to arrange for u and v to be monic in y. The situation is asymmetric and the resultant of u and v with respect to y is $p(x)$. $p'(x)$ can be assumed to be the determinant of the "coefficients" involved in expressing $p(x)$ and y in terms of u and v. $p'(x)$ appears modulo I as the resultant of a pair of a polynomials which are y "coefficients" of u and v in their expressions as members of $\langle p(x), y\rangle$. $p(x)$ and y form a Gröbner basis for I with Jacobian determinant $p'(x)$. Section 1 uses these facts to give several conditions which imply that $p(x)$ is linear or that $p'(x)$ is constant which in turn imply JC for two variables.

Theorem 2.1 involves another set of conditions which imply JC for two variables, related to Proposition 2.1(4) which states that if in the asymmetric situation where u, v are monic in y, the ring $k[x, u, v]$ must $= k[x, y]$, then JC follows. We have that $k[x, y]$ is integral over $k[x, u, v]$ and that the quotient fields of the two rings are equal. The equality of $k(x)[u, v]$ and $k(x)[y]$ as well as the equality of $k[x, u, v]$ and $k[x, y]$ after modding out any linear polynomial in x or appropriately localizing also imply JC for two variables. Most of the results of Section 2 involve conditions which imply the equality of one of the pairs of rings which give JC for two variables. One approach to showing the equality of the rings is to show the conductor is the improper ideal. Theorem 2.5 shows that the conductor as an ideal of $k[x, y]$ is principal and a generator is the image of the partial w.r.t. to X of an element Π which generates the kernel of the obvious map from $k[X, U, V]$, the polynomial ring, onto $k[x, u, v]$. It is also a resultant described in Section 1. Π itself is a determinant of a matrix. One of the main results of the paper is Theorem 2.10 which states that JC for two variables follows if $k[x, u, v]$ must be square-root closed in $k[x, y]$. Proposition 2.11 gives the partial result that $k[u, v]$ is square-root closed in $k[x, y]$. The paper falls short of proving in Section 2.3 that JC for two variables follows if $k[x, y]$ must be seminormal over $k[x, u, v]$ when $j(u, v) = 1$ but Proposition 2.15 describes a special case where this is true. In the case when $k[x, u, v]$ is seminormal in $k[x, y]$, Proposition 2.12 states that one can localize to obtain the situation where there are no modules strictly between the localizations of $k[x, u, v]$ and $k[x, y]$, so in particular y satisfies a monic polynomial of degree two over the localization of $k[x, u, v]$. In fact, even when $k[x, u, v]$ is not seminormal in $k[x, y]$, one can localize to get y satisfying a monic degree-two polynomial over the localization of $k[x, u, v]$ in all but one special case (Proposition 2.16 and the Remark).

Another approach to proving JC for two variables by showing the equality of $k[x, u, v]$ and $k[x, y]$ is to show that $k[x, u, v]$ is normal, which would follow if the generator Π of the kernel from $k[X, U, V]$ onto $k[x, u, v]$ were not contained in the square of any maximal ideal of $k[X, U, V]$. Section 2.4 gives conditions that imply this result. In the special case of $\langle u, v\rangle = \langle p(x), y\rangle$, $\operatorname{res}_y(u, v) = p(x)$, which is square free. Theorem 2.17 shows that if $\operatorname{res}_y(u - a, v - b)$ for any a, b in k is square free, then Π cannot belong to the square of a maximal ideal. It also shows that if $\langle u - a, v - b\rangle$ is a radical ideal of $k[x, u, v]$ for any a, b in k, Π is not in the square of any maximal ideal. These results are taunting since the fact that $k[u, v]$ is unramified in $k[x, y]$ implies that the ideals are radical in $k[x, y]$. Proposition 2.18 shows the ubiquity of the case of trying to show the equality of two rings where the larger is generated over the smaller by an element which satisfies a monic polynomial of degree two as it gives the existence of an intermediate ring between $k[x, u, v]$ and $k[x, y]$ after modding out by $x - a$ for any a in k with that property. The equality of this intermediate ring with $k[x, u, v]/\langle x - a\rangle$ for any a implies JC for two variables.

Sections 1 and 2 are nearly independent of each other as most results of Section 2 only require that the Jacobian pair of polynomials u and v be monic in y. However, nothing is lost in assuming $\langle u, v\rangle = \langle p(x), y\rangle$, and in this case $p(x)$ and $p'(x)$ appear in expressions relating to Π a generator of the kernel of the map from $k[X, U, V]$ onto $k[x, u, v]$, so might provide another avenue to proving that $p(x)$ is linear.

In addition, the paper contains a number of partial results related to the desired conditions. The author apologizes for the myriad of paths but hopes that the paths are worthy of interest and may contribute to a solution of this fascinating problem.

Proposition 0.1. *JC follows if* $\{u_1, \ldots, u_n\} \subseteq k[X_1, \ldots, X_n]$ *with* $j(u_1, \ldots, u_n) = 1$ *implies that the ideal* $\langle u_1, \ldots, u_n\rangle$ *is either nonproper or maximal.*

Proof. Using JC2, this proposition is just the fact that points correspond to maximal ideals over an algebraically closed field. More precisely, if the map from k^n to k^n takes two points to the same point $(a_1, \ldots, a_n)$, then the ideal generated by $\{u_1 - a_1, \ldots, u_n - a_n\}$ is contained in the two maximal ideals corresponding to the two points. Since the Jacobian of $\{u_1 - a_1, \ldots, u_n - a_n\}$ is the same as the Jacobian for $\{u_1, \ldots, u_n\}$, we contradict the assumption that the ideal is maximal. □

Proposition 0.2. *Suppose* $\{F_1, \ldots, F_d\} \subseteq k[X_1, \ldots, X_d]$. *If* $j(F_1, \ldots, F_d) = 1$, *then* $U = \langle F_1, \ldots, F_d\rangle$ *is either nonproper or a radical ideal of* $k[X_1, \ldots, X_d]$ *which is an intersection of a finite number of maximal ideals of* $k[X_1, \ldots, X_d]$.

Proof. This is a consequence of the well-known fact that the extension $k[X_1, \ldots, X_d]$ is unramified over $k[u_1, \ldots, u_d]$ [Ab]. □

Thus, the problem becomes one of showing that the number of maximal ideals involved must be just one.

Theorem 0.3. *Let* $\{u_1, \ldots, u_n\} \subseteq k[X_1, \ldots, X_n]$ *with* k *an algebraically closed field of characteristic* 0. *If* $j(u_1, \ldots, u_n) = 1$ *and* $J = \langle u_1, \ldots, u_n\rangle$ *is a proper ideal, then there exists a change of variables such that* $\langle u_1, \ldots, u_n\rangle = \langle p(X_1), X_2, \ldots, X_n\rangle$ *for some* p *in* $k[X_1]$. *We can assume that* $p(0) = 0$.

Proof. Let $J = M_1 \cap \cdots \cap M_d$ with $M_i = \langle X_1 - c_{i1}, \ldots, X_n - c_{in}\rangle$. First consider an arbitrary linear change of variables $X' = AX$ where X is the column n-tuple of X_i and A is an invertible n by n matrix with entries in k. Let c_i be the column vector determined by $\{c_{ij}\}$. Since k is infinite, A can be chosen so its first row as a vector is not perpendicular to each of the finite number of difference vectors $c_i - c_j$ with $i \neq j$. Thus, $\{Ac_i\}$ has distinct first components. Now, J is a zero dimensional, radical ideal which is in normal position with respect to X'_1 which means $M_i = \langle X'_1 - c'_{i1}, \ldots, X'_n - c'_{in}\rangle$ with distinct $\{c'_{i1}\}$. Since X'_1 is the first component of AX, and $X'_1 - c'_{i1} \in M_i$ iff $c'_{i1} = Ac_i$, we have a set of variables which are in normal position with respect to X_1, dropping the prime notation. By [BW, Proposition 8.77], U has a Gröbner basis of the form $\{p(X_1), X_2 - g_2(X_1), \ldots, X_n - g_n(X_1)\}$. The change of variables $X'_i = X_i - g_i(X_1)$ for $i > 1$ with $X'_1 = X_1$ has the desired form. The last claim follows by exchanging the variable X_1 by any linear factor of $p(X_1)$. □

Of course $\langle u_1, \ldots, u_d\rangle = \langle p(X_1), X_2, \ldots, X_n\rangle$ is maximal iff $\deg p(X_1) = 1$.

The following proposition is the result of adapting an argument of David Wright's. It obtains some reduction in degree involving the variable X_1 and preserves lack of 1–1-ness at the origin.

Theorem 0.4. *If JC is false, there exists a counterexample with the property that* $U = \langle u_1, \dots, u_n \rangle = \langle p(X_1), X_2, \dots, X_n \rangle$ *where the monomials occurring in* u_i *have total degree* $\leqslant 3$ *in* $\{X_i\}$ *for* $i > 1$ *and* $\leqslant 2 \deg p(X_1) - 1$ *in* X_1.

Proof. $k[X_1, \dots, X_n]$ as a k-vector space over k has vector space basis $\{(X_1)^i p(X_1)^j m_k$ where $0 \leqslant i < \deg p(X_1)$ and m_k is a standard monomial in $\{X_i \mid i > 1\}$. We show we can assume the u_i involve only basis terms of the forms $\{x_i x_j x_k$ (with i, j, and k distinct), $(X_1)^i p$, $(X_1)^i X_k$ (with $i < \deg p$), pX_k, or monomials of degree $< 3\}$. If there is a counterexample there is one where the polynomials have degree $\leqslant 3$ and are linear in each variable [BCW]. The proof of Theorem 0.3 involves a change of variables which preserves monomials in X_i with $i > 1$. Thus, it remains only to prove the reduction in degree for basis terms involving X_1. The problem is to reduce the degree while preserving $\langle \{u_i\} \rangle = \langle p(X_1), X_2, \dots, X_N \rangle$ for some N. For monomials involving two or more p's, add X_{n+1} and X_{n+2}. Let $u_{n+1} = X_{n+1} + (X_1)^i p$ and $u_{n+2} = X_{n+1} + p^{j-1} m_k$ where some $(X_1)^i p^j m_k$ appears in say u_m. Replacing u_m with $u_m - c u_{n+1} u_{n+2}$, where c is the appropriate coefficient, reduces the number of monomials with exponent as high as j on p. By iteration we obtain a set of u_i whose monomials are linear in p. For basis terms involving one p, some X_j with $j > 1$ and of degree > 3 (counting p as a factor of degree one for this purpose), the procedure just described can split the monomial by splitting p from X_j. The only basis terms that cannot be reduced or made linear in p and $\{X_i\}$ are of the form $X_k p$, $(X_1)^i p$, and $(X_1)^i X_j$ with $i < \deg p$. $\square$

Corollary 0.5. *If there is a counterexample to JC, there are* u_i *with* $j(u_1, \dots, u_n) = 1$, $\langle u_1, \dots, u_n \rangle \subseteq \langle q(X_1), X_2, \dots, X_n \rangle$ *where* $q(X_1)$ *is of degree two,* u_i *are all of degree* $\leqslant 3$ *and linear in* $q(X_1)$ *and* $\{X_i\}$ *with* $i > 1$.

Proof. Assume a counterexample exists. By Proposition 0.3, we may assume that the variables generate the ideal $\langle p(X_1), X_2, \dots, X_n \rangle$ for some $p(X_1)$ of degree > 1. Choose a degree-two factor, $q(X_1)$, of $p(X_1)$ and repeat the proof above with $q(X_1)$ in place of $p(X_1)$. $\square$

1. The special polynomial $p(X_1)$ in the case of two variables

We assume the following setup throughout the remainder of this section.

$$\left.\begin{array}{l} j(u,v) = 1, \qquad u = \alpha p + \beta y, \qquad p = Fu + Gv, \\ \langle u, v \rangle = \langle p(x), y \rangle, \qquad v = \gamma p + \delta y, \qquad y = Hu + Kv, \\ \text{where we may assume that } \{\alpha, \gamma\} \subseteq k[x] \text{ and that } \deg_y F < \deg_y v = n \text{ and} \\ \deg_y G < \deg_y u = m. \text{ We will see that } u \text{ and } v \text{ are monic in } y \text{ (Proposition 1.1).} \\ \operatorname{res}_y(f,g) = \text{the resultant of } f \text{ and } g \text{ in } k[x,y] \text{ w.r.t. } y. \end{array}\right\} \quad (1)$$

Proposition 1.1. *There exists a change of variables such that u and v can be assumed to be monic in y.*

Proof. Use the Noether normalization trick, i.e., replace x by $x + y^j$ for $j \gg 0$. □

Proposition 1.2. *Given the setup of* (1) *above,* $\operatorname{res}_y(u, v) = p(x)$ *up to a multiple by $\varphi \in k^*$ and* $\operatorname{res}_y(\beta, \delta) = p'(x)$ *modulo $p(x)$ again up to a multiple by $\varphi \in k^*$.*

Proof. Since $\langle u, v\rangle = \langle p(x), y\rangle$, $p(x) \in \langle u, v\rangle$. Further, u and v have a common factor exactly when $p(x) = 0$, namely, y. Thus, $p(x) \mid \rho(x) = \operatorname{res}_y(u, v)$, say $\rho(x) = p(x)h(x)$. Further, the roots of $h(x)$ must also be roots of $p(x)$ since the only maximal ideals, $\langle x - a, y - b\rangle$, that contain u and v, must have $b = 0$ and $x - a$ a factor of $p(x)$. The resultant $\rho(x)$ can be written as $cu + dv$ with $\deg_y c < n$ and $\deg_y d < m$. The coefficients of c and d in $k[x]$ are cofactors of the first column of the resultant matrix,

$$N = \begin{bmatrix} \alpha p & \beta_0 & \beta_1 & \dots & & 1 & 0 & \dots & \dots & 0 \\ 0 & \alpha p & \beta_0 & \beta_1 & \dots & & 1 & 0 & & \\ 0 & 0 & \alpha p & \beta_0 & \dots & & & 1 & & \\ & & & & & & & & 0 & 0 \\ 0 & & \dots & & 0 & \alpha p & & & & 1 \\ \gamma p & \delta_0 & \delta_1 & \dots & & & 1 & 0 & \dots & 0 \\ 0 & \gamma p & \delta_0 & \delta_1 & \dots & & & 1 & 0 & \\ & & & & & & & & & 0 \\ 0 & & & & \gamma p & & & & & 1 \end{bmatrix}.$$

The resultant matrix N is constructed as in [Wa].

Since $p(x) = Fu + Gv$ and u and v have no common factors, $h(x)Fu + h(x)Gv = cu + dv$ implies that $c - h(x)F$ is divisible by v. A degree argument implies that $c - h(x)F = 0 = d - h(x)G$. Thus, $h(x)$ divides the first column cofactors of N. We claim that $h(x) = \varphi$. If not, let $(x - a)$ be a factor of $h(x)$ which is also necessarily a factor of $p(x)$. Expand the determinant of N by the first column to obtain $\rho(x) = \pm p(x)(\alpha\delta_0 - \gamma\delta_0)C$ modulo $p(x)^2$ where C is the determinant of the matrix which results from N by eliminating the first two columns and the first and $(n + 1)$st rows. Thus, $h(x) = \pm(\alpha\delta_0 - \gamma\delta_0)C$ modulo $p(x)$. From $j(u, v) = 1$, one obtains $(\alpha\delta_0 - \gamma\beta_0)p'(x) = 1$ modulo $p(x)$ so that $(x - a) \mid C$. One can observe from N that $C = \operatorname{res}_y(\beta, \delta)$ modulo $p(x)$ so that $(x - a) \mid \operatorname{res}_y(\beta, \delta)$. Modulo $x - a$ if $(y - b) \mid \beta$ and δ then $(y - b) \mid u$ and v so $b = 0$. This implies that $u_y(a, 0) = v_y(a, 0) = 0$, which is a contradiction. Thus, $h(x) = \varphi$ and $\rho(x) = \varphi p(x)$.

To see the second claim, note that p can be factored out of the first column of N so the resulting matrix N^* has determinant φ. Working modulo p, and expanding by the first column of N^* gives $\varphi = \pm(\alpha\delta_0 - \gamma\beta_0)C$ where C is as above. Since modulo $p(x)$, $C = \operatorname{res}_y(\beta, \delta)$ and $j(u, v) = 1$ implies $(\alpha\delta_0 - \beta\delta_0)p'(x) = 1$ modulo $\langle p(x), y\rangle$, $C = \varphi p'(x)$ modulo $\langle p(x), y\rangle$ since they are both inverses of the same element in $k[x, y]/\langle p(x), y\rangle$ up to a nonzero constant φ. □

Remark. We replace p by φp, α by α/φ, and γ by γ/φ so that we can assume $\operatorname{res}_y(u,v) = p(x)$ and $\operatorname{res}_y(\beta,\delta) = p'(x)$ modulo $p(x)$.

Proposition 1.3. *If $j(u,v) = 1$ with $J = \langle u, v\rangle = \langle p(x), y\rangle$ implies that $p'(x)$ is constant modulo $p(x)$, JC follows.*

Proof. $p'(x) = \varphi + m(x)p(x)$ implies that $m(x) = 0$ by comparing degrees. Since $\operatorname{ch} k = 0$, $p'(x) \in k^*$, so $p(x)$ is linear and the result follows from Proposition 0.1 and Theorem 0.3. $\square$

Proposition 1.4. *With β and δ as in* (1)*, if $j(u,v) = 1$ implies $\langle \beta, \delta\rangle = \langle 1\rangle$, JC follows.*

Proof. This follows immediately from Propositions 1.2 and 1.3 since $\operatorname{res}_y(\beta,\delta) \in k^*$. $\square$

1.1. More relations involving $p'(x)$

Proposition 1.5. *Given the setup of* (1)*, we may also assume the following.*

$$\left.\begin{array}{l}\begin{array}{lll} F = p'\delta + Lp, & H = -\gamma p' + Ly, & FK - GH = p', \\ G = -p'\beta + Mp, & K = \alpha p' + My, & \langle F, G\rangle = \langle 1\rangle, \end{array}\\ \text{where } \deg_y L < n\ (= \deg_y v) \text{ and } \deg_y M < m\ (= \deg_y u)\text{. Further, } F \text{ and } G\\ \text{can be assumed to be the polynomials in } y \text{ with coefficients in } k[x] \text{ that result}\\ \text{from the cofactors of the first column of the resultant matrix for } u \text{ and } v \text{ viewed}\\ \text{as polynomials in } y \text{ with coefficients in } k[x]. \end{array}\right\} \tag{2}$$

Proof. Let F and G be the polynomials derived from the resultant matrix so that $Fu + Gv = p$ from Proposition 1.2 and the following remark. Necessarily their degrees in y are less than n and m, respectively. Let $A = F - p'\delta$ and $B = G + p'\beta$. Then $Au + Bv = p - pp'(\alpha\delta - \beta\gamma) = p(1 - p'(\alpha\delta - \gamma\beta)) \in p\langle p, y\rangle = p\langle u, v\rangle$ from the expression of $j(u,v) = 1$. Thus, $Au + Bv = pLu + pMv$. Since v is monic, we can assume that $\deg_y L < \deg_y v$. Then $(A - pL)u = (pM - B)v$. Since u and v have no common factors, $A - pL = Ev$ and $pM - B = Eu$. A degree argument shows that $E = 0$. Thus, $A = pL$, $B = pM$, so $F = p'\delta + pL$ and $G = -p'\beta + pM$ and the relations in the first column hold. To see the relations in the second column, it suffices to define H and K as shown and prove that $Hu + Kv = y$:

$$Hu + Kv = (-\gamma p' + Ly)u + (\alpha p' + Mp)v = y[p'(\alpha\delta - \beta\gamma) + Lu + Mv].$$

Thus, it suffices to show that the bracketed expression is 1. $Fu + Gv = p$ gives $p[p'(\alpha\delta - \gamma\beta) + Lu + Mv] = p$, so we obtain the H, K relations.

Before proving $FK - GH = p'$, note: $\deg_y F = \deg_y \delta = n - 1$ with $\deg_y L \leqslant n - 1$, $\deg_y G = \deg_y \beta = m - 1$ with $\deg_y M \leqslant m - 1$, $\deg_y H \leqslant n$, $\deg_y K \leqslant m$, and recall that we are assuming that $m \leqslant n$.

Apply Cramer's rule to the system:

$$Fu + Gv = p, \qquad Hu + Kv = y$$

to obtain $(FK - GH)u = Kp - Gy$. If $\deg_y(FK - GH) \geqslant 1$, we obtain a contradiction since $\deg_y(Kp - Gy) \leqslant m$. Thus, $FK - GH \in k[x]$. Setting $y = 0$ gives $(FK - GH)\alpha p = K(x, 0)p = \alpha p' p$, so $FK - GH = p'$.

That $\langle F, G\rangle = \langle 1\rangle$ is immediate from $Fu + Gv = p$, $FK - GH = p'$, and that $\langle u, v\rangle = \langle p(x), y\rangle$ is a radical ideal, so p and p' have no common roots. $\square$

Proposition 1.6. *If the relation $AF + BG = 1$ can be accomplished with $\deg_y A \leqslant G$ and $\deg_y B \leqslant F$, and F and G are as in* (1)*, then the corresponding u and v cannot be a counterexample to JC.*

Proof. From $pAF + pBG = p = uF + vG$, we obtain $(pA - u)F = (v - pB)G$. Since F and G have no common factors, we have $pA - U = GD$ and $v - pB = FD$. However, $v - pB$ is monic in y since $\deg v = n > \deg F \geqslant \deg B$. Thus, F must be pseudomonic in y. Since $F = p'\delta + pL$ from Proposition 1.5, we obtain that p' is constant modulo p, and we do not obtain a counterexample from Proposition 1.3. $\square$

1.2. The role of Gröbner bases in realizing $\langle p(x), y\rangle = \langle u, v\rangle$

$\{p(x), y\}$ form a Gröbner basis w.r.t. a term ordering for the ideal $\langle u, v\rangle$. $j(u, v) = 1$ while $j(p(x), y) = p'(x)$. Define an *elementary* operation as a step in the computation of a Gröbner basis yielding $\langle u, v\rangle = \langle z, w\rangle$ and giving generators $\{u + rv = z,\ v = w\}$ or $\{u = z,\ v + su = w\}$ of $\langle u, v\rangle$.

Proposition 1.7. *Assume the setup* (1)*. If $\{p(x), y\}$ can be obtained from $\{u, v\}$ as a basis for $\langle u, v\rangle$ using only elementary operations or, more generally, if there exists an algorithm for obtaining a Gröbner basis such that each basis consists of two elements $\{z, w\}$ with $j(z, w) = 1$ modulo $\langle u, v\rangle$ then JC follows.*

Proof. $\{p(x), y\}$ is a Gröbner basis for $\langle u, v\rangle$ with lex order. It suffices to prove the more general result. This follows from $p'(x) = 1$ modulo $\langle u, v\rangle$ by Proposition 1.3. $\square$

2. Two-variable case of JC and the special intermediate ring, $R = k[x, u, v] \subseteq S = k[x, y]$

The following gives notation and conventions used throughout this section. The reader will need to refer to this list for statements of results.

(1) $\{u, v\} \subseteq k[x, y]$ with u, v polynomials monic in y and $j(u, v) = 1$.
(2) $u = \alpha p + \beta y$, $v = \gamma p + \delta y$ with p, α, γ in $k[x]$. Most results are independent of $\langle u, v\rangle = \langle p(x), y\rangle$, but the assumption gives relations involving $p(x)$ and $p'(x)$.
(3) $R = k[x, u, v] \subseteq S = k[x, y]$, $T = k[X, U, V]$, $R' = k(x)[u, v]$, $S' = k(x)[y]$, $T' = k(X)[U, V]$, $R^* = R/\langle x - a\rangle$, $S^* = S/\langle x - a\rangle$, and $T^* = T/\langle X - a\rangle$ where a is an arbitrary element of k.
(4) Upper case letters will be used for elements of T, T', and T^* and their images under the obvious map τ in R, R', and R^* in lower case.
(5) Π represents a generator of $\operatorname{Ker}\tau : T \to R$ or $T' \to R'$ or $T^* \to R^*$. In general, the same symbols will be used for elements in R, R', R^*, etc.
(6) C, C', and C^* are conductors of R, R', and R^* in S, S', and S^*.
(7) $\Pi_1 = \partial\Pi/\partial X$, $\Pi_{11} = \partial^2\Pi/\partial X^2$ with π_1 and π_{11} being respectively their images in R.

(3)

We show in the following sections that to prove $k[u, v] = k[x, y]$ it suffices to prove that the intermediate ring $k[x, u, v] = k[x, y]$ and give a number of conditions implying this equality.

2.1. Relations between R and S as well as R' and S'

Lemma 2.1. *Let k be a field of characteristic 0, f and g polynomials in $k[y]$ with y an indeterminate. If $\langle f', g'\rangle = \langle 1\rangle$ then $k(f, g) = k(y)$.*

Proof. Suppose the lemma is true for all algebraically closed fields; then for any k, f, and g, there is a finite algebraic extension K of k such that the equality $K(f, g) = K(y)$ is obtained by adjoining the coefficients required to express y as a ratio of polynomials in f and g. By Lüroth's theorem, $k(f, g) = k(\sigma)$ for some σ, so $K(f, g) = K(\sigma)$. Then

$$\begin{aligned}[K : k] &= [K(\sigma) : k(\sigma)] = [K(f, g) : k(f, g)] = [K(y) : k(f, g)]\\ &= [K(y) : k(y)][k(y) : k(f, g)] = [K : k][k(y) : k(f, g)]\end{aligned}$$

so $[k(y) : k(f, g)] = 1$ and $k(y) = k(f, g)$. Thus, we may assume that k is algebraically closed. Suppose that the quotient field of $k[f, g]$ is not $k(y)$. From Lüroth's theorem, $k(f, g) = k(\sigma)$ for some σ in $k(f, g)$. $k(\sigma) = k(1/\sigma)$, so if $\sigma = h/s$ where h and s are in $k[y]$, we may suppose that h and s are relatively prime and that $\deg h \geqslant \deg s$. Further, if $\deg h = \deg s$, we can write σ as $k_0 + r/s$ where $\deg r < \deg s$, so we may assume $\deg h > \deg s$. If $k(\sigma) \neq k(y)$, then $\deg h$ is $\geqslant 2$. We can also assume that h and s are monic. Assume the following:

2. $d\sigma/dy$ has a root which is distinct from a root of s where $\sigma = h/s$.
3. $f(y) = f_1(\sigma)$ and $g(y) = g_1(\sigma)$ where f_1 and g_1 are polynomials.

Then we have $f'(y) = (df/d\sigma)(d\sigma/dy)$ and $g'(y) = (dg/d\sigma)(d\sigma/dy)$. By assumption 2, $d\sigma/dy$ has a root, say $y = d$, which is not a root of s. Thus, by assumption 3,

$df_1/d\sigma$ and $dg_1/d\sigma$ are defined at $y=d$, and $f'(y)$ and $g'(y)$ have the common root $y=d$ contradicting $\langle f', g'\rangle = \langle 1\rangle$.

Proof of 2. Say that $d\sigma/dy$ has a root at $y=a$ if the factor $y-a$ has greater multiplicity in the numerator of $d\sigma/dy$ than in its denominator. First suppose $d\sigma/dy$ has no root; then $(h's-hs')/s^2 = c/m$ where c is a nonzero constant of k. Because h and s are monic of different degrees and $\operatorname{ch} k = 0$, $\deg(h's-hs')$ is $\deg h + \deg s - 1$; so from $(h's-hs')m = cs^2$, $\deg m = \deg s + 1 - \deg h$ follows. Since $\deg h > \deg s$, $\deg m \leqslant 0$. Now, $d\sigma/dy$ is constant, so σ is a polynomial of degree one, contrary to $k(\sigma) \neq k(y)$. Thus $d\sigma/dy$ has a root. If it is not distinct from the roots of s, then $h's-hs'$ has a root common with s which has multiplicity higher than its multiplicity in s^2. Let c be the root, so that $s=(y-c)^t s^*$ where $(y-c) \nmid s^*$. Then

$$h's-hs' = h'(y-c)^t s^* - \bigl(t(y-c)^{t-1}s^* + (y-c)^t s^{*\prime}\bigr)h = (y-c)^{t-1}w$$

where $w = h'(y-c)s^* - ts^*h - (y-c)s^{*\prime}h$. Since $(y-c)$ must be a root of $h's-s'h$ of multiplicity $\geqslant 2t+1$, $(y-c) \mid w$. Therefore, $(y-c) \mid ts^*h$, but t is a nonzero integer and, by hypothesis, $y-c$ divides neither s^* nor h. Thus, $d\sigma/dy$ cannot have a root common with s, so it must have a root which is distinct from the roots of s. □

Proof of 3. We show the result for any $f(y)$ in $k[y]$. Let $f = f_1(\sigma)/f_2(\sigma)$ where f_1 and f_2 are relatively prime. Suppose $f_2(k_0) = 0$ for some k_0. Since $\sigma = h/s$ where $\deg h > \deg s$, we can find a root, d, of $h - k_0 s$, of degree $\geqslant 2$. $y=d$ cannot be a root of s or it would also be a root of h. Thus, we obtain that σ is well defined and equals k_0 at $y=d$. Since f is defined for all values of y, we must have $f_1(k_0)=0$, contradicting the fact that f_1 and f_2 are relatively prime. Thus, f_2 has no roots and, since k is algebraically closed, f_2 is constant. □

Proposition 2.1. *With notation as in* (3), *we have*:

(1) *S is integral over R. In fact, S is the integral closure of R in* q.f.(R).
(2) q.f.(R) = q.f.(S).
(3) *The kernel of the natural map τ from T to R is $\langle \Pi\rangle$ for some Π.*
(4) *If $j(u,v)=1$ implies that $R=S$ or $R'=S'$, or $R^*=S^*$ for any a in k, then $k[u,v]=k[x,y]$ and JC follows.*
(5) *If $j(u,v)=1$ implies that S has a finite projective dimension as an R-module, $R=S$ and JC follows. Similarly, if $j(u,v)=1$ implies that S' has a finite projective dimension as an R'-module, $R'=S'$ and JC follows.*
(6) *If $\Pi \notin M^2$ for any M a maximal ideal of T, then $R=S$ and JC holds. The same result holds for T' and R' as well as T^* and R^* for any a in k.*
(7) *Let Π_1, Π_2, Π_3 denote partials of Π w.r.t. X, U, and V, respectively, in T. In R, we have $\pi_2 = -v_y\pi_1$, $\pi_3 = u_y\pi_1$, and $\pi_1 = -u_x\pi_2 - v_x\pi_3$.*
(8) *π_1, π_2, and π_3 are in the conductor, C, of R in S.*
(9) *In the counterexample context, the conductor ideal, C, has height one.*

(10) *With $u = \alpha p + \beta y$ and $v = \gamma p + \delta y$, $C \subseteq \langle \beta, \delta \rangle$ in S. The equality of R and S can be viewed locally and the obstruction to equality are the maximal ideals containing C. The elements, $U - \alpha p(X)$ and $V - \gamma p(X)$ in T map to βy and δy, respectively, in R. $\Pi \in \langle U - \alpha p, V - \gamma p\rangle$.*

(11) *If $\langle u, v\rangle = \langle p(x), y\rangle$, Π can be assumed to be of the form $p(X) \bmod \langle U, V\rangle$, pseudomonic in U of degree $\deg_y v$ and pseudomonic in V of degree $\deg_y u$. In any case, Π can be assumed to be the determinant of an $m + n$ by $m + n$ matrix which is obtained from lifting the resultant matrix for the monic polynomials that y satisfies over $k[x, u]$ and $k[x, v]$, respectively.*

Proof. (1) Since y generates S over R, it suffices to show that y is integral over R. This follows from the fact that y is a root of $A(Y) = Y^m + \beta_{m-2}Y^{m-1} + \cdots + \beta_0 Y + (\alpha p - u)$. Here β_i is the y^i coefficient of β as a polynomial in y with coefficients in $k[x]$. Since S is a polynomial ring, it is integrally closed in its quotient field, so the second claim follows from part (2).

(2) This follows from Lemma 2.1 by considering the field $k(x)$ and the polynomials u and v in $k(x)[y]$.

(3) T has Krull dimension 3 and R has Krull dimension 2. Thus, the kernel of τ is a height-one prime. Since T is a UFD, the result follows.

(4) If $y \in R$, then y is clearly in $\langle \beta y, \delta y\rangle$ as an ideal of R, from which it follows that $\langle \beta, \delta\rangle = \langle 1\rangle$ in S. Now the result follows from Proposition 1.4. If $R' = S'$, then u and v generate a polynomial ring in one variable over a field. By the famous Abhyankar–Moh result [AM], the degree of the one divides the degree of the other. Let $m = \deg_y u \mid n = \deg_y v$. We may assume that we have a pseudomonic Jacobian pair which gives a counterexample with lowest pair of degrees. Replacing v with $v - u^{n/m}$ gives a Jacobian pair with lower degrees. Since u is pseudomonic in y, it is easy to check that any Jacobian partner is such and we have a contradiction. The case of R^* is essentially the same since we would have $k[u, v] = k[y]$. Since u and v were monic in y, their y degrees remain unchanged modulo $x - a$ and again we have two polynomials generating a polynomial in one variable over a field.

(5) We only argue the case for R. If R is integrally closed then $R = S$ since R and S have the same quotient field and JC follows from part (4). If R is not integrally closed, there exists a maximal ideal M such that R_M is not integrally closed. Choose a maximal ideal, N, of S which lies over M; so since S is integrally closed, we must have $R_M \neq S_N$. Since localization is flat, R_M and S_N satisfy the hypotheses of Theorem 173 of [Ka]. Thus, the grade of S_N equals grade of R_M plus the homological dimension of S_N over R_M. Since the grade of R_M equals grade of S_N in either case (grade 2 in case of R and grade 1 in case of R' as both rings are Cohen–Macaulay of Krull dimensions 2 and 1, respectively), the homological dimension of S_N over R_M is zero; so S_N is a free R_M-module. Since S_N and R_M have the same quotient field, this is impossible unless $S_N = R_M$, and we have a contradiction.

(6) If $\Pi \notin M^2$ for M a maximal ideal of T, T', or T^* then R, R' or R^*, respectively, are regular rings since they are quotients of regular rings by regular elements [Ka]. Thus they are integrally closed; so since S, S', and S^* are the respective integral closures, the claims follow from parts (1) and (4).

(7) Since $\Pi(x,u,v)=0$ in $k[x,u,v]$, we have that $\Pi_1(x,u,v)+\Pi_2(x,u,v)u_x+\Pi_3(u,v,x)v_x=0$ by taking partials with respect to x in $k[x,u,v]$. Taking partials with respect to y gives $\Pi_2(x,u,v)u_y+\Pi_3(x,u,v)v_y=0$. Since $u_xv_y-u_yv_x=1$, the result follows from Cramer's rule.

(8) Since $R\cong T/\langle\Pi\rangle$, R is an affine domain over k and by [Va, Corollary 6.4.1], the Jacobian ideal of R is contained in C. The Jacobian ideal is $\langle\pi_1,\pi_2,\pi_3\rangle$.

(9) In case of a counterexample, C is a proper ideal of R. Since R has Krull dimension two, the height of C is $\leqslant 2$. Since S is finitely generated over R as a module and is contained in q.f.(R), $C\neq 0$. Since R is Cohen–Macaulay, if C is of height two, C contains an R-sequence of length two. In S, we then have polynomials whose resultant as polynomials in $y\neq 0$; so there exists $q\in C$ with $q\in k[x]$. In this case, $R'=S'$, so the result follows by part (4).

(10) Since $k[x,u,v]=k[x,\beta y,\delta y]$, $cy\in R$ implies $c\in\langle\beta,\delta\rangle$. Localizing R at any maximal ideal $m\not\supseteq C$ must imply $y\in R_m$ since $y=(1/c)(cy)$ for any $c\in C-m$. $\Pi\notin k[X]$, so neither is any multiple, and the map from T to R is one-to-one on $k[X]$. Writing Π as $f(X)+\langle U-\alpha p, V-\gamma p\rangle$, since $U-\alpha p$ and $V-\gamma p$ together with X generate T over k, we see that Π maps to $f(x)+\langle\beta y,\delta y\rangle=0$; so $f(X)$ is 0 and the last claim follows.

(11) y is also a zero of $B(Y)=Y^n+\delta_{n-2}Y^{n-1}+\cdots+\delta_0Y+(\gamma p-v)$ over R. δ_i are the y^i coefficients of δ as a polynomial in y. Since $A(Y)$ and $B(Y)$ have the common factor $Y-y$, their resultant is 0. Replacing u by U, v by V, and x by X in $A(Y)$ and $B(Y)$, the determinant, D, of the resultant matrix, M, must be a multiple of Π in T. M is the same as the matrix N in the proof of Proposition 1.2 with αp entries replaced by $\alpha p(X)-U$, γp entries replaced by $\gamma p(X)-V$, and other entries by their capitalizations.

The constant term of D as a polynomial in U and V with coefficients in $k[X]$ is $\mathrm{res}_y(u,v)$ in the variable X; so is $p(X)$ by Proposition 1.2 and Remark. Since $k(x,u,v)=k(x,y)$, while $\{x,u\}$ and $\{x,v\}$ are each algebraically independent pairs over k, we must have that the degree of u over $k(x,v)$ is n since both y and u generate $k(x,y)$ over $k(x,v)$ and y is clearly of degree n. Similarly, the degree of v over $k(x,u)$ must be m. Thus, $D=e\Pi$ with e in $k[x]$. Since the leading coefficient of D in U or V is ±1, $e\in k^*$ and $\langle D\rangle=\langle\Pi\rangle$. □

Since JC implies Proposition 2.1(4)–(6), the following is immediate.

Theorem 2.1. *Let $\{u,v\}\subset k[x,y]$. T.F.A.E.*

(1) *JC for two variables.*
(2) *If $j(u,v)\in k^*$, then $k[x,u,v]=k[x,y]$ or $k(x)[u,v]=k(x)[y]$ or $k[x,u,v]/\langle x-a\rangle=k[x,y]/\langle x-a\rangle$.*
(3) *If $j(u,v)\in k^*$ then $k[x,y]$ has finite projective dimension as a $k[x,u,v]$-module or $k(x)[y]$ has finite projective dimension as a $k(x)[u,v]$-module.*
(4) *If $j(u,v)\in k^*$, then $k[x,u,v]$ is a normal domain.*

2.1.1. $\tau(\partial\Pi/\partial X)=\pi_1$ generates the conductor of R in S and the form of π_1

Computation of $\boldsymbol{\pi_1}$. We know that if $\langle u,v\rangle=\langle p(x),y\rangle$, Π can be written as $CU+DV+p(X)$. This follows from Proposition 1.2 and examining the matrix M in the proof of Proposition 2.1(11) and the fact that modulo $\langle U,V\rangle$, M is the resultant matrix of u and v (with X in place of x). Thus, $\Pi_1=p'(X)+C_1U+D_1V$. $\pi_1=\tau(\Pi_1)=p'(x)$ modulo I where $I=\langle p(x),y\rangle=\langle u,v\rangle$. Now use the product rule for determinants to obtain $\Pi_1=\det M_1$ modulo $\langle U-\alpha p, V-\gamma p\rangle$ where $M_1=M$ with the nonzero entries of the first column replaced by $(\alpha p)'$ and $(\gamma p)'$ and one obtains more, namely that modulo $\langle y\rangle$, $\pi_1=[(\alpha p)'\delta_0-(\gamma p)'\beta_0]\ \mathrm{res}_y(\beta,\delta)=\mathrm{res}_y(\beta,\delta)$ since the expression in brackets is the pure x part of $j(u,v)=1$. This result will be recorded later.

We now record some items defined in the proofs above, specifically of Proposition 2.1(11).

$$\left.\begin{array}{l}\text{$A(Y)$ and $B(Y)$ are the monic irreducible polynomials which have y as a root}\\ \text{over $k[x,u]$ and $k[x,v]$, respectively.}\\[1ex] \quad A(Y)=A^*(Y)(Y-y),\qquad B(Y)=B^*(Y)(Y-y)\quad \text{in } k[x,y][Y].\\[1ex] \quad A(Y)=Y^m+\beta_{m-2}Y^{m-1}+\cdots+(-\beta y),\qquad A^*(Y)=Y^{m-1}+\cdots+\beta.\\[1ex] \quad B(Y)=Y^n+\delta_{n-2}Y^{n-1}+\cdots+(-\delta y),\qquad B^*(Y)=Y^{n-1}+\cdots+\delta.\end{array}\right\}\tag{4}$$

Lemma 2.2. *Let $A(Y)$ and $B(Y)$ be as in* (4)*. Then we have the following.*

(1) *Let $A_T(Y)$ and $B_T(Y)$ be the coefficient lifts of $A(Y)$ and $B(Y)$ in $R[Y]$ to $T[Y]$ by "capitalizing" the expressions in* (4) *rewriting βy and δy as $u-\alpha p$ and $v-\gamma p$. Extend τ from T onto R to $T[Y]$ onto $R[Y]$ by sending Y to Y. We have $\tau(A_{T1}(y))=u_x$, $\tau(B_{T1}(y))=v_x$, $A^*(y)=u_y$, and $B^*(y)=v_y$.*
(2) *$A^*(Y)$ and $B^*(Y)$ are monic relatively prime polynomials in Y with coefficients in S.*
(3) *If $C(Y)$ and $D(Y)$ are such that $A(Y)C(Y)+B(Y)D(Y)=0$ with $\deg_Y C<\deg_Y B$ and $\deg_Y D<\deg_Y A$ and whose coefficients are obtained from the cofactors of the first column of the resultant matrix for $A(Y)$ and $B(Y)$, we must have $C(Y)=fB^*(Y)$ and $D(Y)=-fA^*(Y)$ with f in $k[x,u,v]$.*

Proof. (1) Since $B_T(Y)=Y^n+\delta_{n-2}Y^{n-1}+\cdots+\delta_0Y+\gamma p(X)-V$ and $V_1(\partial V/\partial X)=0$, it is clear that $B_{T1}(Y)$ is v_x in upper case letters, so mapping X to x and substituting y for Y gives the equality. $B^*(Y)=Y^{n-1}+\cdots+q_{n-d}Y^{n-d}+\cdots+\delta$ where $q_{n-d}=y^{d-1}+\delta_{n-2}y^{d-2}+\cdots+\delta_{n-d}$. Thus, if we substitute y for Y in $q_{n-d}Y^{n-d}$, we obtain $y^{n-1}+\delta_{n-2}y^{n-2}+\cdots+\delta_{n-d}y^{n-d}$ and summing from $d=0$ to $d=n-1$, we obtain n copies of y^{n-1}, $n-1$ copies of $\delta_{n-2}y^{n-2},\ldots,n-d+1$ copies of $\delta_{n-d}y^{n-d},\ldots,$ and one copy of δ_0. Since $v=\gamma(x)p(x)+\delta y$, the result is v_y. The results involving A are similar.

(2) Clearly, $A^*(Y)$ and $B^*(Y)$ are monic with coefficients in $k[x,y]$ since $Y-y$, $A(Y)$, and $B(Y)$ are monic. If $A^*(Y)$ and $B^*(Y)$ had a common nontrivial factor $Q(Y)$, then

$A(Y)$ and $B(Y)$ would have a common factor of degree $\geqslant 2$. In this case the same argument that implies that the resultant matrix of $A(Y)$ and $B(Y)$ has determinant 0 can be applied to argue that the matrix constructed in the same manner from $A(Y)$ and $B(Y)$ with two fewer rows and two fewer columns would have determinant 0. By lifting the entries to T, we obtain a matrix whose determinant must be a multiple of Π, which is impossible by a degree argument.

(3) Since $A(Y)$ and $B(Y)$ have a common factor, namely $Y - y$, their resultant is 0. Since, $B^*(Y)A(Y) - A^*(Y)B(Y) = 0 = C(Y)A(Y) + D(Y)B(Y)$, we have $(B^*(Y) - C(Y))A(Y) = (D(Y) + A^*(Y))B(Y)$; so by canceling $Y - y$ multiplicatively and then A^*B^* additively, we obtain $-C(Y)A^*(Y) = D(Y)B^*(Y)$. Because $A^*(Y)$ and $B^*(Y)$ are relatively prime, by a degree argument we must have $C(Y) = fB^*(Y)$ and $D(Y) = -fA^*(Y)$ for some element f in $k(x,u,v) = k(x,y)$. However, $C(Y)$ has coefficients in $k[x,u,v]$ and $A^*(Y)$, $B^*(Y)$ are monic, so $f \in R$ and part (3) holds. $\square$

The following lemma is a partial flatness result for S over R.

Lemma 2.3. *Let $s \in S$. If $f(x) \neq 0$, then $f(x)s \in R$ implies $s \in R = k[x,u,v]$.*

Proof. First we argue that $f(x)s \in k[x,u]$ implies $s \in k[x,u]$. If not, we can assume a counterexample with minimal degree in u. Let $f(x)s = g(x)u^j + w$ where w involves lower degree terms. Since u is monic in y, $f(x) \mid g(x)$. Thus, $f(x) \mid w$ in S. By minimality, $w = f(x)z$ with z in $k[x,u]$. But then $s \in k[x,u]$ and the claim follows. Now write $f(x)s = \sum_0^d t_i v^i$ where $t_i \in k[x,u]$. We can assume that $d \leqslant m-1$ since v is a root of a monic polynomial of degree m over $k[x,u]$ from Proposition 2.1(11). We proceed by induction on the number of factors of $f(x)$. If $f(x) \in k$, the result is trivial. Let a be a root of $f(x)$. If $t_i(a,u) = 0$ for all i, then $t_i \in \langle x - a\rangle$ and we can divide both sides of the expression thus reducing the number of factors. If $t_i(a,u) \neq 0$ for some i, then we obtain a polynomial of degree $\leqslant m-1$ for which $v(a,y)$ is a root over $k[u(a,y)]$. We argue this is not possible since modulo $\langle x-a\rangle$, $k[u,v]$ and $k[y]$ have the same quotient field. Since u is monic of degree m, y clearly has degree m over $k[u]$ modulo $\langle x-a\rangle$. If v generates the quotient field of $k(y)$ over $k(u)$, it must have degree m also. Lemma 2.1 implies that $k[u,v]$ and $k[y]$ have the same quotient field modulo $x-a$. $\square$

Proposition 2.4. *The conductor, C, of R in S is principal as an ideal of S. If $j(u,v) = 1$ implies that C is principal as an ideal of R, R' or R_P for any prime $P \supseteq C$, JC follows.*

Proof. $Ck(x)[y]$ is a principal ideal and can be generated by an element, g, of R with no factors in $k[x] - k$. By Lemma 2.3, we may assume that $g \in C$ in R. If $g \in k^*$, we have $k(x)[u,v] = k(x)[y]$ and $C = \langle 1\rangle$. If $c \in C$, then $c = sg$ where $s \in k(x)[y]$. For some $f(x)$ we have $f(x)s = t \in k[x,y]$, so $f(x)c = tg$. Since $c \in k[x,y]$ and no nonconstant polynomial in x divides g, $f(x) \mid t$ in $k[x,y]$ and $c = sg$ for some s in $k[x,y]$. If C is principal as an ideal of R, $gy = gr$, so $y \in R$. The other claims follow similarly. $\square$

Lemma 2.5.

(1) *$\Pi = Z(U - \alpha p(X)) + W(V - \gamma p(X))$ where $\tau(Z) = \delta f$ and $\tau(W) = -\beta f$ for some Z and W in T and f is as in Lemma* 2.2(3).
(2) *$f = \tau(\partial\Pi/\partial X) = \pi_1$. Further, $\partial\Pi/\partial X = \Pi_1$ is the cofactor of the $(n, 1)$ entry of the matrix, M, whose determinant is Π.*
(3) *$\tau(\partial\Pi/\partial X) = \pi_1$ generates C as an ideal of S.*
(4) *If u and v are as in Section* 1*, namely $\langle u, v\rangle = \langle p(x), y\rangle$, then as a polynomial in y, $\tau(\partial\Pi/\partial X)$'s $= \pi_1$'s constant term is $p'(x)$ modulo $p(x)$ and equals* $\operatorname{res}_y(\beta, \delta)$.

Proof. (1) By Proposition 2.1(11), $\Pi = Z(U - \alpha p) + W(V - \gamma p)$ for Z and W, the $(1, 1)$ and $(n + 1, 1)$ cofactors of the resultant matrix M. By our choice of Z and W, $\tau(Z)$ and $\tau(W)$ are the constant terms with respect to Y of the polynomials $C(Y)$ and $D(Y)$ in Lemma 2.2. By Lemma 2.2, $C(Y) = fB^*(Y)$, whose constant term is $f\delta$, and $D(Y) = -fA^*(Y)$, whose constant term is $-f\beta$.

(2) Let $A(Y)$, $B(Y)$, $C(Y)$, and $D(Y)$ be as in (4) and in Lemma 2.2. Let $A_T(Y)$, $B_T(Y)$, $C_T(Y)$, and $D_T(Y)$, respectively, denote the polynomials lifted to T. We have $\Pi = C_T(Y)A_T(Y) + D_T(Y)B_T(Y)$ where $C_T(Y)$ and $D_T(Y)$ are obtained from the cofactors of the first column of the resultant matrix for $A_T(Y)$ and $B_T(Y)$ whose determinant is Π. See the proof of Proposition 2.1(11). Now, $\Pi_1 = C_{T1}(Y)A_T(Y) + C_T(Y)A_{T1}(Y) + D_{T1}(Y)B_T(Y) + D_T(Y)B_{T1}(Y)$. We have $\pi_1 = C_1(Y)A(Y) + C(Y)A_1(Y) + D_1(Y)B(Y) + D(Y)B_1(Y)$. Replace Y by y to obtain $\pi_1 = C(y)A_1(y) + DG(y)B_1(y)$ since $A(Y)$ and $B(Y)$ have the common root y. $C(Y) = fB^*(Y)$ and $B_1(Y) = -fA^*(Y)$ from Lemma 2.2. However, $B^*(y) = v_y$, $A^*(y) = u_y$, while $B_1(y) = v_x$ and $A_1(y) = u_x$ from Lemma 2.2(1). Thus, $\pi_1 = f(u_xv_y - v_xu_y) = f$. The leading coefficient of $C_T(Y)$ is the $(n, 1)$ cofactor of the resultant matrix for $A_T(Y)$ and $B_T(Y)$ and it therefore maps to the leading coefficient of $C(Y) = \pi_1B^*(Y) = \pi_1$ since B^* is monic.

(3) Let q generate the conductor ideal in S. Consider $f(Y) = qB^*(Y)$ and $g(Y) = -qA^*(Y)$. Recall that $A(Y) = (Y - y)A^*(Y)$ and $B(Y) = (Y - y)B^*(Y)$. $f(Y)$ and $g(Y)$ have coefficients in R. Let $F(Y)$ and $G(Y)$ lift $f(Y)$ and $g(Y)$. Since $[fA + gB](Y) = 0$, we must have $F(Y)A_T(Y) + G(Y)B_T(Y) = L\Pi$ for some L in $T[Y]$ since Π clearly also generates the kernel of the obvious map from $T[Y]$ to $R[Y]$. A_T and B_T are as in the proof of (2) above. Now take the partial derivative of both sides of the expression $FA_T + GB_T$ with respect to X to obtain $F_1A_T + FA_{T1} + G_1B_T + GB_{T1} = L(Y)\Pi_1 + L_1(Y)\Pi$. Map to $R[Y]$ and substitute y for Y to obtain $q(u_xv_y - v_xu_y) = L(y)\pi_1$. ($A_T(y) = B_T(y) = 0$, $F(y) = qB^*(y) = qv_y$, $G(y) = -qu_y$, $A_{T1}(y) = u_x$, and $B_{T1}(y) = v_x$ by Lemma 2.2(1).) Thus, q is a multiple of π_1 in S and the claim follows.

(4) The proof follows the proof of Proposition 2.1(11) under computation of π_1. □

Theorem 2.5. *Let $\langle\Pi\rangle$ be the kernel of the map τ from $T = k[X, U, V]$ to $R = k[x, u, v]$, where u and v are a Jacobian pair monic in the variable y, C the conductor of R in $S = k[x, y]$, Π_1 the partial of Π w.r.t. X. Then*

(1) *$\tau(\Pi_1) = \pi_1$ generates the conductor of R in S as an ideal of S.*

(2) *$\Pi = Z(U-\alpha p)+W(V-\gamma p)$ is a determinant of a resultant matrix M. $\partial\Pi/\partial X = \Pi_1$ is the $(n,1)$ cofactor of M, and $\tau(\partial\Pi/\partial X) = \pi_1$ appears in $\tau(Z) = \delta\pi_1$ with $\tau(W) = -\beta\pi_1$. π_1 necessarily divides the cofactor of each entry of the first column of $\tau(M)$ in $k[x,y]$. Further if $\langle u,v\rangle = \langle p(x),y\rangle$, π_1, as a polynomial in y with coefficients in $k[x]$, has constant term equal to $\mathrm{res}_y(\beta,\delta)$ and this polynomial has the form $p'(x)$ modulo $p(x)$.*

Proof. This is merely a cleanup of Lemma 2.5 given Propositions 2.1(11), 1.2(3) and Lemma 2.2(3) since $f = \pi_1$. □

Remark. A nice proof of Theorem 2.5(1) due to Richard Swan can be given using formulas for the inverse different and conductor from [Se, III-6]. Let A and B be the Dedekind domains $k(x)[u]$ and $k(x)[y] = S'$. Proposition 11 of [Se, III-6] implies that $R'^* = R'/\pi_3$ and that $B^* = S'/u_y$ where $*$ is defined by $D* = \{w \in \text{q.f.}(D) \mid \text{Trace}(wD) \subseteq A\}$, the inverse different. Then Corollary 1 of the same section implies $C' = \pi_3 B^* = \pi_3/u_y S' = \pi_1 S'$ by Proposition 2.1(7). The proof of Proposition 2.4 implies that π_1 also generates C.

2.2. JC follows if R must be square-root closed in S

The notion of seminormality plays a major role in what follows. The definition below is one of several [Sw].

Definition 2.6. R is seminormal in S if $s^2, s^3 \in R$ with s in S implies $s \in R$. In our situation, R seminormal in S implies that the conductor of R in S is a radical ideal.

If A is a one-dimensional Noetherian domain with finite normalization, it is known that A is seminormal in its normalization if and only if the conductor of A is a radical ideal in its integral closure in the total quotient ring. This is cited in the first two lines of [Da] as an immediate consequence of [BM, 7.12] or [E2, 4.3] and [Tr, 3.6]. Thus R' is seminormal iff π_1 is square free.

Lemma 2.7. *y is a root of a monic polynomial over R of degree $\leqslant 2$ iff C can be generated by $\leqslant 2$ elements. The result also holds for any localization of R including R' and for localizations of R^*.*

Proof. Suppose that the monic degree of y is $\leqslant 2$ in the case of R, so that S as a module over R is generated by $\{1, y\}$. Since $C = \langle\pi_1\rangle$ in S, then $C = \langle\pi_1, \pi_1 y\rangle$ in R. If $C = \langle\pi_1 a, \pi_1 b\rangle$ in R, then $\pi_1 = r_1\pi_1 a + r_2\pi_1 b$ implies that $1 = r_1 a + r_2 b$ in S. Since S is integral over R, we must also have $r_1r_3 + r_2r_4 = 1$, so $C = \langle\pi_1 = r_1\pi_1 a + r_2\pi_1 b, -r_4\pi_1 a + r_3\pi_1 b\rangle$ by Cramer's rule. The two generators may be relabeled as $\{\pi_1, \pi_1 a\}$. $\pi_1 a^2 \in C$ so $\pi_1 a^2 = r_5\pi_1 + r_6\pi_1 a$ and since $\pi_1 \neq 0$, a is of monic degree two over R. Now $\pi_1 y = r_7\pi_1 + r_8\pi_1 a$ implies that $y = r_7 + r_8 a$. Thus, a generates S over R and is of monic degree $\leqslant 2$, so it is easily to show that y is also of monic degree $\leqslant 2$. Thus, again S as a module is generated by $\{1, y\}$, so $C = \langle\pi_1, \pi_1 y\rangle$. The other cases are similar. □

We now discuss the seminormal case. Clearly, if R is square-root closed in S, R is seminormal in S. Some of the following results are given with an eye to an eventual proof that one can reduce JC to proving seminormality of R.

Lemma 2.8. *If R is seminormal in S, then R' is seminormal in S'. R^* is seminormal in S^* for all but a finite number of a. If R is square-root closed in S, R' is square-root closed in S'.*

Proof. Assume R is seminormal in S, so π_1 is square free in S by the discussion following Proposition 2.6. $C' = \langle \pi_1 \rangle$ in S' by Lemma 2.3. If π_1 is square free in S, it is also in S' by Gauss's lemma, so R' is seminormal in S'. There is only a finite number of values of a, so $\pi_1(a, y)$ has repeated factors in $k[y]$. Since a generator of C^* must divide π_1's image, it can have no repeated factors in $S^* = k[y]$. Thus R^* is seminormal $k[y]$ in S^* for all but a finite number of values of a.

Suppose that R is square-root closed in S and $(s/f(x))^2 \in R'$ where $s \in S$. Then $g(x)s^2 \in R$ for some $g(x)$. By Lemma 2.3, $s^2 \in R$ and, by hypothesis, $s \in k[x, u, v]$. Thus $s/f(x) \in R'$ and R' is square-root closed in S'. □

Proposition 2.9. *If R is seminormal in S or R' seminormal in S', then y is a root of a monic polynomial of degree $\leqslant 2$ over R'. If R^* is seminormal in S^*, y is a root of a monic polynomial of degree $\leqslant 2$ over R^*.*

Proof. Either of the hypotheses implies that C' can be generated by $\{\pi_1, \pi_1 y\}$. Further, C^* can be generated by $\{c^*, c^* y\}$ in R^* with a chosen to preserve seminormality and $C^* = c^* S^*$. This follows immediately from Theorem 2.5 and the fact that the inverse image of the conductors in question to T' or T^*, both of which are polynomial rings in two variables over a field, are intersections of maximal ideals, so are generated by two elements [Va, Theorem 4.24]. Now Lemma 2.7 applies. □

Theorem 2.10. *With $\{u, v\} \subset k[x, y]$, JC in two variables is equivalent to: if $j(u, v) \in k^*$, then $k[x, u, v]$ is square-root closed in $k[x, y]$, or $k(x)[u, v]$ is square-root closed in $k(x)[y]$, or $k[x, u, v]/\langle x - a \rangle$ is square-root closed in $k[x, y]/\langle x - a \rangle$.*

Proof. One direction is trivial. That $k[x, u, v]$ is square-root closed implies that $k(x)[u, v]$ is square-root closed, so we argue the latter case. Now, we have that $k(x)[u, v]$ is seminormal in $k(x)[x, y]$, so by Proposition 2.9 we have that $y^2 + ry$ is in $k(x)[u, v]$ with $r \in k(x)[u, v]$. Thus, $(y + r/2)^2 \in k(x)[u, v]$ and since $k(x)[u, v]$ is square-root closed in $k(x)[y]$, we have $y + r/2 \in k(x)[u, v]$, so $y \in k(x)[u, v]$ and the result follows from Proposition 2.1(4). The argument for $k[x, u, v]/\langle x - a \rangle$ is similar. □

Proposition 2.11. *$k[u, v]$ is square-root closed in $k[x, y]$ only under the assumption that $j(u, v) = 1$.*

Proof. First suppose that $s^2 = f$ where f is irreducible in $k[u, v]$. Since $j(u, v) = 1$, we have that u and v are algebraically independent and $k[u, v]$ is a polynomial ring. Now

$2ss_x = f_2u_x + f_3v_x$ and $2ss_y = f_2u_y + f_3v_y$ where f_2, f_3 are partials with respect to u and v, respectively. Since $j(u,v) = 1$, we have $\langle f_2, f_3\rangle = \langle ss_x, ss_y\rangle \subseteq \langle s\rangle$ in $k[x,y]$. Thus, $s \mid f_2$ and f_3, so in $k[u,v]$, $f = 0$ implies $s = 0$, so $f_2 = f_3 = 0$. By the Hilbert Nullstellensatz, $\{f_2, f_3\}$ is contained in the radical of $\langle f\rangle$ in $k[u,v]$. Since f is irreducible, $f \mid f_2$ and f_3, but this is impossible by a degree argument.

Now if $s \in k[x,y]$ is such that $s^2 = f \in k[u,v]$ with $s \notin k[u,v]$, suppose that $s^2 = f = p_1 \dots p_d$ where the p_i are possibly nondistinct irreducible elements of $k[u,v]$ and d is least. If some p_i reoccurs, then writing $p_i = q_1 \dots q_k$ where the q_i are irreducible in $k[x,y]$, we have $s = p_i t$ in $k[x,y]$ and $s^2 = p_i^2 t^2$ in $k[u,v]$. If $t \in k[u,v]$, so is $s = p_i t$, so we may assume that $t \notin k[u,v]$, but t^2 in $k[u,v]$ contradicts the minimality of number of irreducible factors in $k[u,v]$. Thus, we may assume that s^2 is a product of distinct irreducible elements of $k[u,v]$.

By the result in the first paragraph of this proof, we may assume that no irreducible factor of s^2 in $k[u,v]$ is a square in $k[x,y]$. Thus, there is some q, an irreducible factor of s in $k[x,y]$, which must divide two distinct irreducible factors of s^2 in $k[u,v]$, say p_1 and p_2. Since q generates a prime ideal of $k[x,y]$, its intersection with $k[u,v]$ is a prime ideal containing both p_1 and p_2. Since both generate a prime ideal of $k[u,v]$ and are distinct, the ideal has height two, so is maximal. Since k is algebraically closed, the intersection ideal is of the form $\langle u-a, v-b\rangle$ for some a, b in k. Then q divides both $u-a$ and $v-b$ in $k[x,y]$, so q divides $j(u-a, v-b) = j(u,v) = 1$, yielding a desired contradiction. □

2.3. The seminormal case and reduction to the case where y satisfies a monic polynomial of degree at most two

If $R \neq S$, $R' \neq S'$, or $R^* \neq S^*$, the inequalities will be preserved by localizing the situation at any prime containing the conductor. In the seminormal case, the following result indicates in the case of a counterexample that the localizations are as close as they can be without being equal.

Proposition 2.12. *Let R be seminormal in S and assume that u, v in R give our counterexample.*

(1) *Let $m' \supseteq C'$ be a maximal ideal of R', then $m'R'_{m'}$ is the conductor of $R'_{m'}$ in $S'_{A'}$ where $A' = R' - m'$ and there are no $R'_{m'}$ submodules properly between $R'_{m'}$ and $S'_{A'}$.*
(2) *Let a be such that $R^* = R/\langle x-a\rangle$ is seminormal in $S^* = S/\langle x-a\rangle$ and let $m^* \supseteq C^*$ be a maximal ideal of R^*. We have that $m^*R^*_{m^*}$ as the conductor of $R^*_{m^*}$ is in $S^*_{A^*}$ with $A^* = R^* - m^*$ and there are no $R^*_{m^*}$ submodules properly between $R^*_{m^*}$ and $S^*_{A^*}$.*

Proof. R' is seminormal since R is. R' is a factor ring of a regular ring by a regular element, so R is Gorenstein. Then $R'_{m'}$ is a one-dimensional Gorenstein local ring with finite integral closure $S'_{A'}$ with $A' = R' - m'$ [Ka]. Further, $R'_{m'}$ is seminormal as this property is preserved by localization [Sw]. By a theorem of Rush [Ru, Theorem 6] and the proof, if $R'_{m'}$ is not $S'_{A'}$, the conductor of $R'_{m'}$ in $S'_{A'}$ is $m'R'_{m'}$ and there are no proper $R'_{m'}$ submodules between $R'_{m'}$ and $S'_{A'}$. Thus, (1) holds. The proof of (2) is similar. □

Lemma 2.13. *Assume that R' (R^*) is seminormal in S' (S^*). Then*

(1) *there exists s of the form $y + r$ with r in R' (R^*) such that $s^2 \in R'$ (R^*).*
(2) *$\langle \pi_1, s\rangle = S'$ in S' and $\langle \pi_1, s^2\rangle = R'$ in R'. $\langle c, s\rangle = S^*$ in S^* and $\langle c, s^2\rangle = R^*$ in R^* where $\langle c\rangle = C^*$. ($\pi_1 = \tau(\partial\Pi/\partial X)$.)*

Proof. The existence of such an element in S' has been observed in the proof of Theorem 2.10, so (1) holds. For (2), since S' is a PID, we need only show that π_1 and s are relatively prime. Write $\pi_1 = q_1 \dots q_k$ with q_i distinct irreducibles in S' by seminormality. If s and π_1 are not relatively prime, let q_{some} be their gcd and let $\pi_1 = q_{\text{some}} q_{\text{rest}}$. Since $s = y + r$ clearly generates S' over R' and $s^2 \in R'$, we have $S' = R' + R's$. Write $q_{\text{rest}} = r_1 + r_2 s$. Then $s q_{\text{rest}} = s r_1 + r_2 s^2$. Since $s^2 \in R'$ and $s q_{\text{rest}} \in \pi_1 S'$, $r_1 s \in R'$. Then, $r_1 \in C' = \pi_1 S'$. Now we have $q_{\text{rest}} \mid r_1$, so $q_{\text{rest}} \mid r_2 s$ from $q_{\text{rest}} = r_1 + r_2 s$. However, q_{rest} is relatively prime to s, so $q_{\text{rest}} \mid r_2$ and we obtain that $r_2 s$ is in R', since it must be in $\pi_1 S'$. Again this implies that $r_2 \in \pi_1 S'$. Now $\pi_1 \mid q_{\text{rest}}$ provides a contradiction unless q_{some} is a unit and the claim follows. The proof for R^* and S^* is similar. □

Lemma 2.14. *If R is seminormal in S, then $C \cap k[u, v]$ is a nonzero principal radical ideal.*

Proof. Since R is algebraic over $k[u, v]$, $C \cap k[u, v] \neq 0$. If R is seminormal in S, C is a radical ideal and $C \cap k[u, v] = C''$ is a radical ideal with height $\geqslant 1$. Further, C has height one in R. If C'' had height two, then some maximal ideal, $\langle u - a, v - b\rangle$, in $k[u, v]$ would be a minimal prime over C'', so $= \text{Ann}(g) \bmod C''$ with $g \notin C''$. Then $g(u - a) \in C''$ and $g(v - b) \in C''$. Thus $g(u - a) = \pi_1 f$ and $g(v - b) = \pi_1 h$. Since $\pi_1 \nmid g$, $u - a$ and $v - b$ have a common factor in S which is not possible since $j(u - a, v - b) = 1$. Thus, height of C'' is 1 so C'' is principal since it is a radical ideal in a polynomial ring. □

Recall that we are attempting to prove JC by showing $R = S$, which will follow if $\tau(\partial\Pi/\partial X) = \pi_1 \in k^*$. In fact, by a degree argument, $\pi_1 \in k^*$ iff $\partial\Pi/\partial X = \Pi_1 \in k^*$. One approach is to show that $\partial^2\Pi/\partial X^2 = \Pi_{11}$ is 0 or equivalently that $\tau(\partial^2\Pi/\partial X^2) = \pi_{11} = 0$.

Proposition 2.15. *Let R' be seminormal in S'. Then we cannot have a counterexample to JC if $\tau(\partial\Pi/\partial X) = \pi_1$ and $\tau(\partial^2\Pi/\partial X^2) = \pi_{11}$ have a common nontrivial factor in S'.*

Proof. By Lemma 2.13, there exists $s = y + r$ with r in R' with s^2 in R', then let $e = \pi_1 s$, $f = s^2$ with e and f in R. We show that $e_1 = \tau(E_1) \in C'$. We have $E^2 - F\Pi_1^2 = G\Pi$ because in R', $e^2 = s^2\pi_1^2 = f\pi_1^2$. Taking partials of the former with respect to X we have that in R', $2ee_1 - f_1\pi_1^2 - 2f\pi_1\pi_{11} = g\pi_1$ so $2s\pi_1 e_1 = f_1\pi_1^2 + 2f\pi_1\pi_{11} + g\pi_1$. Thus, canceling π_1, we have $e_1 s \in R'$. Since $S' = R' + R's$ and C' is a radical ideal, $e_1 \in C'$ as claimed.

Since π_1 has no nontrivial factors in $k[x]$, a common factor in S exists iff it does in S'. We work initially in S and suppose that such a factor q exists. We can assume that q is irreducible in S, so qS is a prime ideal of S. Let $P = qS \cap R$. No nonzero element of $k[x]$ is in P. Localize R at P and T at $\tau^{-1}(P)$. Since R_P is a further localization of R', e_1 is in the conductor of R_P in S_{R-P}. $C' = \langle \pi_1, y\pi_1 \rangle = \langle \pi_1, \pi_1(y+r) = \pi_1 s = e \rangle$, so $\{\pi_1, e\}$ generates the conductor of R_P in S_{R-P}. Let $\tau^{-1}(P) = P^*$. T_{P^*} is a further localization of T' and $\tau^{-1}(C)T_{P^*} = (P^* \cap Q)T_{P^*}$ where in T', P^* is a maximal ideal, Q is an intersection of maximal ideals, and $P^* \cap Q = \tau^{-1}(C)$. Since $P^* \cap Q = P^*Q$ and $\tau^{-1}(C) = \langle \Pi_1, E, \Pi \rangle$, we must have $\{\Pi_1, E, \Pi\}$ generating $P^*T_{P^*}$, which we will abbreviate as P^* in the following. P^* is a differential ideal under the differential map D which takes a partial derivative with respect to X. This follows from the fact that each of the generators maps into P^* under D and the product/sum rules. Write Π as $W_0(U,V) + \cdots + W_d(U,V)X^d$. By iterating D d times, we have $W_d(U,V)$ in P^*, and subtracting the X^dth term from Π and repeating the argument, we obtain that $W_i(U,V)$ is in P^* for all i. Thus, the W_i are in $P^{**} = P^* \cap k[U,V]$ in T_{P^*}. $P^* \cap k[U,V]$ is height one because τ is one-to-one if restricted to $k[U,V]$, and $\tau(P^*)$ has height one by Lemma 2.14. Thus, P^{**} is principal. Say, its generator is $H(U,V) \in k[U,V]$ and is irreducible. Thus, there exists $G_i \in T - P^*$ such that the $G_i W_i$ are in HT. Then $H \mid W_i$ in T and necessarily in $k[U,V]$. Since Π is irreducible, this is a contradiction unless H is a unit. However, H being a unit implies that $C = R$ and we do not have a counterexample. □

Proposition 2.16. *If $\tau(\partial\Pi/\partial X) = \pi_1$ has an irreducible factor in S which does not divide $\tau(\partial^2\Pi/\partial X^2) = \pi_{11}$, then there is a minimal prime P of R over $\langle \pi_1 \rangle$ such that y is a root of a monic polynomial of degree $\leqslant 2$ over R_P.*

Proof. Let $d = y\pi_1$. Then $d^2 = (y^2\pi_1)\pi_1 = n\pi_1$ for some n in R. Then $D^2 - N\Pi_1 = M\Pi$ in T and taking partials w.r.t. X we have $2DD_1 - N_1\Pi_1 - N\Pi_{11} = M_1\Pi + M\Pi_1$ in T and $2dd_1 - n_1\pi_1 - n\pi_{11} = m\pi_1$. Canceling π_1 yields $2d_1 y - n_1 - y^2\pi_{11} = m$, so $\pi_{11}y^2 - 2d_1 y \in R$. Let $q(y) \mid \pi_1$ but not π_{11} in S and let $P = q(y)S \cap R$. Clearly, P is a minimal prime over C if C is proper and $\pi_{11} \notin P$, so $y^2 - (2d_1/\pi_{11})y \in R_P$ with $2d_1/\pi_{11} \in R_P$. □

Note that, as a result of Propositions 2.15 and 2.16, the only situation where we have not yet concluded that y is a root of a monic polynomial of degree $\leqslant 2$ over some localization of R is the case where π_{11} is in the radical of the ideal $\langle \pi_1 \rangle$ with R not seminormal.

2.4. Results relevant to showing that $R = k[x,u,v]$ must be a regular ring

The results in this section give conditions which imply JC because they imply Proposition 2.1(6), namely that $\Pi \notin M^2$ for M a maximal ideal of T, T', or T^* with notation as in (3).

Theorem 2.17. *Assume as usual that u and v are monic in the variable y.*

(1) *If $j(u,v) = 1$ implies that $\langle u-a, v-b \rangle$ is a radical ideal of $R = k[x,u,v]$ for all a, b in k then JC follows.*
(2) *If $j(u,v) = 1$ implies that $\mathrm{res}_y(u-a, v-b)$ is a square-free polynomial in x for all a, b in k, then JC follows.*

Proof. (1) If $\Pi \in M^2$ for some maximal ideal M of T, then we have $\Pi = (X-a)^2F + (U-b)G + (V-c)H$ for some a, b, c in k and elements F, G, H of T where $M = \langle X-a, U-b, V-c\rangle$. We can assume $F \in k[X]$. Then in R, $(x-a)^2 f(x) \in \langle u-b, v-c\rangle$. Since $\langle u-a, v-b\rangle$ is a radical ideal, $(x-a)f(x) \in \langle u-b, v-c\rangle$ in R. But then in T, there is a multiple of Π whose pure X part is $(X-a)f(X)$, which is not possible.

(2) We show that $\Pi \notin M^2$ where $M = \langle X', U', V'\rangle$ with $X' = X-a$, $U' = U-b$, and $V' = V-c$. Since x', u', and v' generate R with u' and v' a Jacobian pair monic in y, all previous results apply to the primed variables and in fact we can drop the primes. Now the result follows by noting that the resultant matrix whose determinant is Π is of the form $q(X)$ modulo $\langle U, V\rangle$ with $q(x) = \mathrm{res}_y(u, v)$. If $\Pi \in M^2$ then $X^2 \mid q(X)$, contradicting our hypothesis. $\square$

Remark. Of course, $u-a$ and $v-b$ form a Jacobian pair since u and v do so. Thus, $\langle u-a, v-b\rangle$ is a radical ideal of $k[x, y]$, so a product of the irreducible factors of $\mathrm{res}_y(u-a, v-b)$ does belong to $\langle u-a, v-b\rangle$, but it is not hard to find examples showing that this fact is insufficient to prevent multiplicity in the resultant. Thus, the Jacobian condition needs to be involved in a substantial way if one wants to establish the square-freeness of the resultant.

Proposition 2.18. *If $\Pi \in M^2$ for $M = \langle X-k_1, U-k_2, V-k_3\rangle$ in T, then there is a test element, d, in $S^* = S/\langle x-k_1\rangle$ such that*:

(1) *$d^2 + k_0 d \in R^* = R/\langle x-k_1\rangle$ for some element k_0 of k.*
(2) *$\langle u-k_2, v-k_3\rangle$ is contained in the conductor of R^* in $R^*[d] \subseteq S^*$.*
(3) *If $\Pi \in M^3$, then d^i is also in R^* for all $i \geqslant 2$; but*
(4) *$R^* = R^*[d]$ gives a contradiction.*

Proof setup. In this paragraph, we work in R. Let $x' = x-k_1$, $u' = u-k_2$, $v' = v-k_3$. Since $\Pi \in M$, $\tau(M) = m = \langle x', u', v'\rangle$ is maximal in R. Let $\langle x', y' = y-e\rangle$ lie over m, so $u' = \beta' y' + x'\alpha'$ and $v' = \delta' y' + x'\gamma'$, where we may assume that α' and γ' are in $k[x']$ and y' generates S over R. The change of variable to x' and the Jacobian pair $\{u', v'\}$ generate the same R over k; so that Proposition 2.1(11) implies that we can realize Π in terms of X', U', and V' as an $m+n$ by $m+n$ determinant whose constant term as a polynomial in U' and V' maps to $\mathrm{res}_y(u', v')$ in R. If $\Pi \in M^2$, we have:

(i) $\Pi = AU' + BV' - X'^2\Sigma'$ with Σ' in $k[X]$.
(ii) $au' + bv' = x'^2\sigma'$ where $\sigma' \in k[x]$.
(iii) $a = a_1u' + a_2v' + a_3x'$.
(iv) $b = b_1u' + b_2v' + b_3x'$. (Here subscripts are not partial differentiation.)
(v) $su' + tv' = x'\sigma'$ with s and t in S.
(vi) $a - sx' = dv'$ and $b - tx' = -du'$ for some d in S.

(i)–(iv) are clear. (v) follows because $\langle u', v'\rangle$ is a radical ideal of S. (vi) follows from (ii), (v), and the fact that u' and v' are relatively prime.

(1) and (2). In this and subsequent paragraphs we work in R^* but we use the same symbols for elements as in R. After substituting 0 for x' in the expressions for a and b in (iii), (iv), and (vi) we obtain:

$$a_1u' + (a_2 - d)v' = 0, \qquad (b_1 + d)u' + b_2v' = 0$$

in R^*. Since u' and $v' \neq 0$, the determinant of the above system of equations is 0, so $a_1b_2 - (a_2 - d)(b_1 + d) = 0$ and d is a root of a monic polynomial of degree two over R^*, namely $X^2 + (b_1 - a_2)X + (a_1b_2 - a_2b_1)$. Since u' and v' both multiply d into R^*, we have that $d^2 + k_0d \in R^*$ for some $k_0 \in k$ and (1) holds for the element d. Further, since $\langle u', v'\rangle$ multiply d into R^*, the conductor of R^* in $R^*[d] \supseteq \langle u', v'\rangle$, so (2) holds.

(3) If $\Pi \in M^3$ with $M = \langle X', U', V'\rangle$, then $\Pi = AU' + BV' - \Sigma X'^3$ with $A, B \in M^2$ and $\Sigma' = X'\Sigma$ with notation as in (i) of the proof setup. Working in R^*, since the a_i and b_i of (iii) and (iv) can be assumed to be in $\tau(M) = \langle u', v'\rangle$, we have $d^2 \in R^*$ from the relation $d^2 + (b_1 - a_2)d + (a_1b_2 - a_2b_1) = 0$. Since $dv' \in \langle u', v'\rangle^2$ in R^*, $d \in \langle u', v'\rangle$ in S^* and $d^2 \in R^* \cap \langle u', v'\rangle S^*$. Since $\langle u', v'\rangle$ is maximal in R^*, $d^2 \in \langle u', v'\rangle$, so $d^i \in R^*$ for all $i \geqslant 2$.

(4) If $R^*[d] = R^*$, $d = r + x'z \in S$, $r \in R$, and $z \in S$. a (from (iii)) $= x's + rv' + x'zv'$, so $x'(s + v'z) \in R$ and by Lemma 2.3, $s + v'z \in R$. Similarly, b (from (iv)) $= x't - ru' - x'u'z$ and $x'(t - zu') \in R$, so $t - zu' \in R$. Then $(s + zv')u' + (t - zu')v' = su' + tv' = x'\sigma'$. Since the coefficients of the leftmost expression are in R, there exists $LU' + MV' - X'\Sigma' \in k[X', U', V']$ which is a multiple of Π, what is impossible since $X'^2\Sigma'$ is the pure X' part of Π. □

If $R^* = R/\langle x - k_1\rangle$ is seminormal, then by (3) $d \in R^*$ when $\Pi \in M^3$ and since R^* is seminormal for all but a finite number of x', we have the following.

Corollary 2.19. *If R is seminormal in S, then $\Pi \in M^3$ for at most a finite number of maximal ideals, M, of T.*

Proof. Assuming the counterexample case by Lemma 2.8, $R/\langle x - k_1\rangle$ can only fail to be seminormal for a finite number of $k_1 \in k$. By (3) and (4) above, Π is not in any M^3 where $X - k_1 \in M$ and $R/\langle x - k_1\rangle$ is seminormal. Therefore, if $\Pi \in M^3$ with $M = \langle X - k_1, U - k_2, V - k_3\rangle$, $R/\langle X - k_1\rangle$ fails to be seminormal. $\Pi_1 \in M$ and an ideal of T which $\supseteq \langle X - k_1, \Pi, \Pi_1\rangle$ must be of height 3 since $\langle(\Pi, \Pi_1\rangle$ has height two and we may assume that no element of $k[X]$ is in $\langle \Pi, \Pi_1\rangle$ by Proposition 2.1(4). Thus, there is only a finite number of maximal ideals $M \supseteq \langle X - k_1, \Pi, \Pi_1\rangle$ and the claim follows. □

3. Concluding remarks

The paper provides two main avenues to approach JC in two variables. Despite the initial hope that one might be able to show $p'(x) \in k^*$ when $j(u, v) \in k^*$ and $\langle u, v\rangle = \langle p(x), y\rangle$, it seems that whenever some mathematical quantity ought to belong to k^* in order for JC to hold, the quantity was $p'(x)$. The other main avenue involves showing $k[x, u, v] = k[x, y]$

or equality after taking appropriate localizations or quotients. It would be of interest to show the equality in case y satisfies a monic polynomial of degree two over $k[x,u,v]$. Showing that $k(x)[u,v] = k(x)[y]$ when y satisfies a monic polynomial of degree two over $k(x)[u,v]$ gives that JC reduces to proving that $k(x)[u,v]$ is seminormal in $k(x)[y]$ which is implied by the seminormality of $k[x,u,v]$ in $k[x,y]$. Mild assumptions give localizations where y is monic of degree two but this author was not able to take advantage of the low degree.

References

[Ab] S.S. Abhyankar, Expansion Techniques in Algebraic Geometry, in: Lecture Notes in Math., Vol. 146, Springer-Verlag, Berlin and New York, 1970.

[AM] S.S. Abhyankar, T.T. Moh, Embeddings of the line in the plane, J. Reine Angew. Math. 276 (1975) 148–166.

[BCW] H. Bass, E. Connell, D. Wright, The Jacobian conjecture: reduction of degree and formal expansion of the inverse, Bull. Amer. Math. Soc. 7 (1982) 287–330.

[BM] H. Bass, M.P. Murthy, Grothendieck groups and Picard groups of abelian group rings, Ann. of Math. (2) 86 (1967) 16–73.

[BW] T. Becker, V. Weispfennig, Gröbner Bases, Cambridge Univ. Press, Cambridge, 1993.

[Da] E. Davis, On the geometric interpretation of seminormality, Proc. Amer. Math. Soc. 68 (1978) 1–5.

[E2] S. Endo, Projective modules over polynomial rings, J. Math. Soc. Japan 15 (1963) 339–352.

[Ka] I. Kaplansky, Commutative Rings, Allyn and Bacon, 1970.

[Ru] D. Rush, Seminormality, J. Algebra 67 (1980) 377–384.

[Se] J.-P. Serre, Local Fields, Springer-Verlag, 1979.

[Sw] R. Swan, On seminormality, J. Algebra 67 (1980) 210–229.

[Tr] C. Traverso, Seminormality and Picard groups, Pisa Sc. Norm. Sup. Ann. Ser. 3 24 (1978) 585–595.

[Va] W. Vasconcelos, Computational Methods in Commutative Algebra and Algebraic Geometry, Springer-Verlag, 1998.

[vdE] A. van den Essen, Polynomial Automorphisms and the Jacobian Conjecture, in: Progr. in Math., Vol. 190, Birkhäuser, 2000.

[Wa] R. Walker, Algebraic Curves, Dover, 1950.